NSTISSAM INFOSEC 3-00
August 2000

Advisory Memorandum on Web Browser Security Vulnerabilities

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01082000	N/A	-

Title and Subtitle Advisory Memorandum on Web Browser Security Vulnerabilities	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es) NSTISSC	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms IATAC COLLECTION	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 9	

National Security Telecommunications and Information Systems Security Committee

National Manager

FOREWORD

1. Virtually all major Web browsers have significant security flaws, making it possible for hackers to attack. These attacks run the gamut from simple denial of service, through theft of files and personal information, to full-fledged system penetration permitting the attacker to delete files, insert viruses, change information, and leave hidden monitoring programs. But Web browsers offer tremendous convenience and productivity advantages and their use will only accelerate in both industry and government.

2. This NSTISSAM outlines some of the steps you can take to lower your risk when browsing the Web and discusses the benefits and consequences of the security measures.

3. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this instruction at the address listed below.

4. Comments and suggestions regarding this NSTISSAM may be directed to the NSA Information Systems Security Policy and Doctrine Division, telephone (410) 854-6815 or DSN 244-6815.

MICHAEL V. HAYDEN
Lieutenant General, USAF

NSTISSC Secretariat (I42). National Security Agency.9800 Savage Road STE 6716. Ft Meade MD 20755-6716
(410) 854-6805.UFAX: (410) 854-6814
nstissc@radium.ncsc.mil

SECTION I – INTRODUCTION

1. Browsing the Web can be a dangerous proposition. Virtually all major Web browsers have significant security flaws, making it possible for hackers to attack you when you visit a Web page that contains malicious content. Despite the opportunities for attackers, the risks of browsing the Web are not as great as they might appear. For one thing, attackers cannot choose the time and place of the attack, but must wait for a victim to come to their Web page. This makes it difficult for attackers to target specific users unless they have information about the user's browsing habits. Also, despite the fact that almost all browsers have serious vulnerabilities, for the most part they are different vulnerabilities. So, attackers have to choose the attack that fits the browser, a task that requires a moderate level of sophistication on the attacker's part. Finally, since it is difficult to focus attacks narrowly, it is likely that serious attacks will get discovered relatively quickly.

2. Although the use of a Web browser puts the machine the browser is on at some risk, it also offers tremendous convenience and productivity advantages. Use of the Web as the standard interface to information sources and enterprise applications is a trend that will only accelerate in both industry and government. In most environments, it is simply not reasonable to say "security at all costs" and give up the huge advantages that the Web offers. Consequently, users must weigh the convenience and capabilities that Web browsers provide against the risks that they pose. The purpose of this paper is to list the most important steps that you can take to lower the risk of Web browsing, and to summarize the pros and cons of taking each of those steps. Most of the steps decrease your security risk, but most also require time and effort, and many diminish some of the advantages that the Web provides. So the costs and benefits need to be evaluated on a case-by-case basis.

SECTION II - SCOPE

3. The following paragraphs, arranged roughly in order of the security benefit the steps provide, outline some of the steps that you can take to lower your risk when browsing the Web. Note that this is not the same as the order of benefit-to-cost ratio, which will be different for each organization. As a result, these steps should not be taken as recommendations, but rather as options to consider for your particular security environment.

a. Avoid browsing from systems with sensitive data:

If you have a few systems that contain highly sensitive information and others that are much less critical, one option is to prohibit Web browsing from the sensitive systems. An extreme example of this is a system that contains classified information. Obviously, no user should ever browse the unclassified Web from such a system. The advantage of this approach is that it limits Web-client attacks to the less sensitive systems. The disadvantage is that users on the more sensitive systems may find it inconvenient to physically walk to the systems that have Web access, and may find it time consuming (and thus, expensive) to move information or resources back and forth between the sensitive system and the WWW. Furthermore, unless the sensitive systems have no network connectivity to the Web systems, there is still the possibility of a sophisticated attack that uses the system with the Web browser as an entry point into the more sensitive systems.

b. Use Mosaic or another older browser:

Since most of the attackers focus on Netscape or Internet Explorer and since many of the attack mechanisms depend on scripting languages, plugins, or other active content, an older and simpler browser such as Mosaic (http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/) involves less risk than a more capable browser. Of course, Mosaic also offers less convenience, since many Web-based activities depend on the advanced capabilities that the newer browsers provide.

c. Update browser releases frequently:

While it is generally good advice to keep operating systems and general software applications patched and up-to-date, it is especially important for Web browsers to be upgraded to later releases. If your site has a fast network connection and an automated tool for software configuration and installation, this step offers significantly increased security at relatively little cost. Both Netscape and Microsoft offer free versions of their latest browsers from:

http://home.netscape.com/download/index.html
http://www.microsoft.com/windows/ie/download/defult.asp

The 128-bit encryption products will provide stronger encryption for Web applications than the 56-bit or 40-bit products. Microsoft advises that fraudulent email messages containing supposed patches have been circulated; they only deliver patches through their Web site.

d. Be careful how you browse the Web:

- Be judicious when giving out personal information in Web forms.
- Be extremely cautious of downloading software components and executables. Today's cool screen-saver could be tomorrow's virus.
- Avoid browsing the Web as a privileged user; for example, on a Unix system do not run a browser when logged in as "root."
- Be mildly suspicious of links to unknown sites.

e. Disable unnecessary browser plugins, especially Microsoft Office:

A browser plugin is a software application that handles a particular type of document. For example, when you follow a link to a PDF file, most browsers automatically pass the file to the Adobe Acrobat plugin. In many cases, content is automatically passed to the plugins without the user's consent or knowledge. That means that each and every plugin is an additional potential source of attack. In fact, many of these plugins have been shown to have extremely serious security vulnerabilities. For example, the Microsoft Office plugin in Internet Explorer 3 and 4 can be exploited to let an attacker run arbitrary code on the client machine. Even though other plugins have not had such significant flaws identified, it makes sense to disallow plugins that you don't normally need. When you decide to download a new plugin, or for that matter any software for your computer, make sure you download it from a reputable source.

Disabling Plugins on Netscape:

1. From the menu bar select "Edit->Preferences".
2. Select the "Applications" item from the tree at the left.
3. A scrolling list of various document types will appear on the right.

4. To remove a particular plugin highlight it and press the "Remove" button. Alternatively, you can click the "Edit" button and tell Netscape to inform you whenever it would run this particular plugin. This way you would at least be notified if a Web page tried to send you a document in an clandestine fashion.
5. When you are done editing or removing extraneous plugins click the "OK" button at the bottom of the dialog window.
6. Note: You can enter the URL "about:plugins" to gain some information about plugins you may have.

Disabling Plugins on Internet Explorer:

See the following section on disabling Active-X components. The procedure for disabling plugins in Internet Explorer is exactly the same.

f. Turn Off Active-X:

Active-X is a powerful and useful technology from Microsoft that lets software components be reused in a variety of applications. Internet Explorer comes bundled with Active-X support; Netscape requires a separate (nonstandard) plugin. The problem in the Web context is that Active-X components have complete access to the client system. So, if you allow one in, it can do anything it wants to your system. Although Active-X supports digital signatures to verify the source of the component, it takes a moderately sophisticated user to check out the source of the component and the source of the Web page that is applying the component. As a result, some organizations prefer to disable Active-X rather than trust their users to only allow safe components.

Disabling Active-X Components on Internet Explorer:

1. From the menu bar select "View->Internet Options". A dialog window will pop-up.
2. Select the "security" tab from the top.
3. In the pull-down list of options, select "Internet Zone".
4. Below, select the "Custom" security level checkbox.
5. Click on the "settings" button. A scrolling list will pop-up.
6. Scroll down until you see the "Active-X and Plug-ins" section. There may be five or so different sub-sections in which you should select "Disable" in order to completely turn off all Active-X components.
7. Click the "OK" button at the bottom of the "Settings".
8. Click on the "OK" Button at the bottom of the dialog window.

g. Turn off JavaScript and VBScript:

Scripting languages such as JavaScript have been a ripe source of security flaws in Web browsers. Many browser-based attacks stem from the use of a scripting language in combination with some other security flaw. For example, attacks that let Web sites steal files from client machines typically result from a combination of the fact that JavaScript can automatically submit forms with some bug in the way file upload form fields are initialized. There are also a variety of well-known attacks where JavaScript assists in the process of fooling users into thinking they are at trusted sites and thus giving away private information to attackers. On the other hand, a large number of sites depend on JavaScript, and disabling it will make these sites less usable, or, in some cases, completely unusable.

Disabling JavaScript for Netscape:

1. From the menu bar select "Edit->Preferences". A dialog window will pop-up.
2. Select the "Advanced" tab from the options on the left.
3. Deselect the checkbox labeled "Enable JavaScript".
4. Deselect the checkbox labeled "Enable JavaScript for Mail and News" (if present).
5. Click the "OK" button at the bottom of the dialog window.

Disabling JavaScript for Internet Explorer:

1. From the menu bar select "Edit->Internet Options". A dialog window will pop-up.
2. Select the "Security" tab from the top.
3. In the pull-down list of options, select "Internet Zone".
4. Below, select the "Custom" security level checkbox.
5. Click on the "Settings" button. A scrolling list will pop-up.
6. Scroll down until you see the "Scripting" section. Under "Active Scripting" select "Disable" and "Disable Scripting of Java Applets".
7. Click on the "OK" button at the bottom of the "Settings'".
8. Click on the "OK" button at the bottom of the dialog window.

h. Turn Off Java:

Java applets are programs written in the Java programming language that can be run in Web browsers. Applets might be used to add graphical drawings to a Web page or to act as a user interface to server-side programs. Java has a large number of security safeguards intended to prevent attacks, and has typically been one of the stronger links in the chain of Web browser security features. Nevertheless, several Java-based attacks have been demonstrated on various platforms by researchers, and disabling Java is an option that extremely security-conscious sites might want to take after performing the other steps first. If you leave Java enabled and run on Windows or Unix, make sure that the environment variable CLASSPATH is not set when the browser is launched. This variable refers to directories containing trusted Java classes that are, on most browsers, executed with relaxed security restriction.

Disabling Java Applets for Netscape:

1. From the menu bar select "Edit->Preferences". A dialog window will pop-up.
2. Select the "Advanced" tab from the options at the left.
3. Deselect the checkbox labeled "Enable Java".
4. Click the "OK" button at the bottom of the dialog window.

Disabling Java Applets for Internet Explorer:

1. From the menu bar select "View->Internet Options". A dialog window will pop-up.
2. Select the "Security" tab from the top.
3. In the pull-down list of options, select "Internet Zone".
4. Below, select the "Custom" security level checkbox.
5. Click on the "Settings" button. A scrolling list will pop-up.
6. Scroll down until you see the "Java" section. Select "Disable Java".
7. Click the "OK" button at the bottom of the 'Settings'.
8. Click the "OK" button at the bottom of the dialog window.

i. Turn Off Cookies:

Have you ever noticed how some Web sites greet you by name when you visit them? Often this is accomplished by a technology known as cookies that let a Web server record some information on your PC's hard disk. This information (such as a unique user ID) is then resent to the Web server every time your browser requests a page from that site. This lets the site remember what you did on their site previously, and, if you explicitly provided them personal information, lets them associate that information with you when you visit their site in the future. This is extremely useful in many contexts: a site can remember the stocks or sports teams you want to see, can automatically display weather for your location, and can remember your password or credit card number. Although cookies are not a significant security risk (they can't be used to insert viruses or fill up your disk), they can be a serious privacy risk in some contexts. For example:

- Cookie data is not encrypted and therefore anybody with access to your hard disk can view your cookies. This is a problem if poorly designed sites use the cookies to store sensitive data, rather than using an innocuous user ID which is only associated with real data on the server.
- Although most reputable e-commerce companies have explicit privacy statements, companies could share or exchange cookie information without a user's knowledge, giving a third party indirect access to your personal information.
- By loading images from the same cooperating third party, two different sites can share cookies. This could let one site gain information about what you did at a different site. Netscape has a setting that still allows cookies but prevents this problem, but Internet Explorer does not.

Disabling Cookies in Netscape:

1. From the menu bar select "Edit->Preferences". A dialog window will pop-up.
2. Select the "Advanced" tab from the option at the left.
3. Select the checkbox labeled "Only accept cookies originating from the same server as the page being viewed". To turn off cookies completely select "Do not accept or send cookies".
4. Click the "OK" button at the bottom of the dialog window.

Disabling Cookies in Internet Explorer:

1. From the menu bar select "View->Internet Options". A dialog window will pop-up.
2. Select the "Security" tab from the top.
3. In the scrolling-list of options, look in the "Security" section.
4. Click the "OK" button at the bottom of the dialog window.

SECTION III - MORE INFORMATION REGARDING WEB SECURITY SITES

4. The following URLs are a good starting place to remain informed about Web browser security issues:

a. Netscape Security Site:

http://www.netscape.com/security/

b. Internet Explorer Security Site:

http://www.microsoft.com/window/ie/security/default.asp

c. World Wide Web Consortium's Client-side Security Site:

http://www.w3.org/Security/faq/wwwsf7.html

d. Princeton's Secure Internet Programming Laboratory:

http://www.cs.princeton.edu/sip/

e. Computer Emergency Response Team (not focused on client security issues):

http://www.cert.org/tech_tips/

SECTION IV - SUMMARY

5. Browsing the Web opens your system up to a variety of serious attacks. Almost every browser and operating system combination is vulnerable, but it is very difficult for hackers to focus their attack on you, and the likelihood of attack is quite small. There are a number of steps you can take to decrease your vulnerability, all of which require some level of time and effort and some of which limit the usefulness of the Web in various ways. Sites should evaluate the risks based on their local criteria and decide which steps are appropriate for their systems.

SECTION V - ACKNOWLEDGEMENT

6. The development of this Advisory Memorandum, a collaborative effort with Johns Hopkins University Applied Physics Laboratory, is gratefully acknowledged and appreciated.